UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/613,750	07/03/2003	Liqun Chen	B-5154 621086-5	5657

7590 05/15/2007

Hewlett-Packard Company
Intellectual Property Administration
3404 E. Harmony Road
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
05/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/613,750	CHEN ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-49* is/are pending in the application.

4a) Of the above claim(s) *3,6,13-24,36-38 and 45-47* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,5,7-12,25-29,32-35,39-41,43,44 and 49* is/are rejected.

7)☒ Claim(s) *30,31,42 and 48* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/27/03 & 1/20/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The IDS of 10/27/03 & 1/20/04 were received and considered.

2. The response of 3/12/07 was received and considered.

3. Claims 1-49 are pending.

4. Claims 3, 6, 13-24, 36-38 & 45-47 are withdrawn as being directed to a non-elected species.

Election/Restrictions

5. Applicant's election of Species I and V in the reply filed on 3/12/2007 is acknowledged. Because applicant did not distinctly and specifically point out the supposed errors in the restriction requirement, the election has been treated as an election without traverse (MPEP § 818.03(a)).

Claim Objections

6. Claims 1-2, 4-5, 7-12, 25-27 & 39-42 are objected to because of the following informalities:

a. Regarding claim 1, "generating" (line 1) should be replaced with "generate".

b. Regarding claim 1, "data set" (line 4) should be replaced with "data set that".

c. Regarding claim 11, "is arranged form" (line 1) should be replaced with "is arranged to form".

d. Regarding claim 25, "second data set" (line 2) should be replaced with "second data set that".

e. Regarding claim 39, "two said" (line 1 and line 2) should be replaced with "two of said".

f. Regarding claim 40, "two said" (line 1) should be replaced with "two of said".

g. Regarding claim 41, "two said" (line 1) should be replaced with "two of said".

7. Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claim 27 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

h. Regarding claim 27, the limitation "the encryption key" (line 1) lacks sufficient antecedent basis. For the purposes of this Office Action, the above limitation is understood to read "the cryptographic key".

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this

subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. Claims 25-27, 34-35, 39-41, 44 & 49 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication 2003/0179885 to Gentry et al. (**Gentry**).

Regarding claim 25, Gentry discloses generating a cryptographic key (recipient secret element, $S_{z(n+1)}$, i.e. the private key of the recipient, ¶90) using a first data set (ID_2 ,¶86) that corresponds to a first identifier (ID_2 is identity information associated with the ancestral PKG 304(b), ¶¶85-86 ¶86 which is used in the creation of P_2, used in ¶88 to create $S_{z(n+1)}$), a second data set (P_2, ¶88) which corresponds to a first trusted party's public key (P_2 is the public element of ancestral PKG 304(b), ¶86, used in ¶88 to create $S_{z(n+1)}$), a third data set (ID_3, ¶86) that corresponds to a second identifier (ID_3 is identity information associated with the ancestral PKG 304(d), ¶¶85-86 ¶86 which is used in the creation of P_3, used in ¶88 to create $S_{z(n+1)}$) and a fourth data set (P_3, ¶88) which corresponds to a second trusted party's public key (P_3 is the public element of ancestral PKG 304(d), ¶86, used in ¶88 to create $S_{z(n+1)}$).

Regarding claim 26, Gentry discloses encrypting a fifth data set (message) with the cryptographic key (secret element, encrypting/signing a message using the sender's (which is the same as the recipient in ¶¶85-95) secret element, ¶143).

Regarding claim 27, Gentry discloses a method of generating a cryptographic key (key to recover V, i.e. $\prod_{i-2}^{n+1} \hat{e}(Q_{i-1}, U_i)$ where $U_i = rP_{zi}$, ¶95) using a first data set ($U_i = rP_{zi}$,¶86) that corresponds to a first identifier ($P_{zi} = H_1(ID_1,...,ID_{zi})$, ¶86), a second data set that corresponds to a first trusted party's public key (ancestor's key generation parameter, Q_{i-1}, ¶89), a third data set

($U_i = rP_{zi}$ for the next ancestral PKG, ¶86) and a fourth data set that corresponds to a second party's public key (next ancestor's key generation parameter, Q_{i-1}, ¶89), wherein the cryptographic key is formed using a Tate or Weil pairing operating (pairing function ê, ¶64 & ¶66 & $\prod_{i-2}^{n+1} \hat{e}(Q_{i-1}, U_i)$, ¶95) on the first and second data sets ($\hat{e}(Q_{i-1}, U_i)$, *i*=first value, ¶95) and the third and fourth data sets ($\hat{e}(Q_{i-1}, U_i)$, *i*=next value, ¶95).

Regarding claim 34, Gentry discloses a method of generating a cryptographic key (key to recover V, i.e. $\prod_{i-2}^{n+1} \hat{e}(Q_{i-1}, U_i)$ where $U_i = rP_{zi}$, ¶95) wherein a bilinear mapping function (pairing function ê, ¶64 & ¶66) is used to process multiple data sets each comprising data related to a respective associated of trusted authority and user identity (Q-value key generation parameter from authority, which equals the authority's secret times the root public element, ¶89 and P_{zi} which is the public element of the PKGs, ¶86). Note that multiple data sets are achieved from $i-2$ to $n+1$, ¶95.

Regarding claim 35, Gentry discloses wherein the cryptographic key is an encryption key (key to recover V, i.e. $\prod_{i-2}^{n+1} \hat{e}(Q_{i-1}, U_i)$ where $U_i = rP_{zi}$, ¶95), each data set comprising an identity-based public key (P_{zi}, ¶86) derived from said user identity ($P_{zi} = (H_1(ID_1,...,ID_{zi}), 1 \le i \le n)$, ¶86), and a public key element of the trusted authority (PKG) that is based on a secret of the latter (Q-value key generation parameter from authority, where $Q_{zi} = s_{zi}P_o, 1 \le i \le n$, ¶89, where s_{zi} is the authority's (PKG's) secret, ¶87).

Regarding claims 39-41, Gentry discloses wherein at least two said data sets relate to different user identities ($U_i = rP_{zi}$, $i-2$ to $n+1$, ¶95) and at least two said data sets relate to different trusted authorities ($Q_{zi} = s_{zi}P_o, 1 \le i \le n$, where s_{zi} is the particular authority's (PKG's) secret, ¶87 & ¶95).

Regarding claim 44, Gentry discloses wherein there are *n* data sets (corresponding to the levels in Gentry, i.e. $i-2$ to $n+1$ in ¶95) and the encryption key is generated as $\prod_{1}^{n} p(R_{TAi}, rQ_{IDi})$ (see ¶95, $\prod_{i-2}^{n+1} \hat{e}(Q_{i-1}, U_i)$) where p() is said bilinear mapping function (pairing function ê, ¶64 & ¶66), Q_{IDi} is the identity-based public key associated with the i^{th} data set (value generated for particular lower level PKG, P_{zi} is the identity of the PKG at that level, ¶86), R_{TAi} is the public key element of the trusted authority associated with the i^{th} data set (value generated for particular lower level PKG, $Q_{zi} = s_{zi}P_o, 1 \le i \le n$, where s_{zi} is the ancestral authority (PKG) of that level's authority (PKG's) secret, ¶87 & ¶95) and *r* is a random number (random encryption parameter, ¶95).

Regarding claim 49, Gentry discloses wherein the bilinear mapping function (pairing function ê, ¶64 & ¶66) is one of a Tate pairing and a Weil pairing (¶64).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 1-2, 4-5, 7-12, 28-29, 32-33 & 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Gentry**, in view of U.S. Patent Application Publication 2003/0182554 to Gentry et al. (**Gentry '554**).

Regarding claim 1, Gentry discloses generating a cryptographic key (recipient secret element, $S_{z(n+1)}$, i.e. the private key of the recipient, ¶90) using a first data set (ID_2,¶86) that corresponds to a first identifier (ID_2 is identity information associated with the ancestral PKG 304(b), ¶¶85-86 ¶86 which is used in the creation of P_2, used in ¶88 to create $S_{z(n+1)}$), a second data set (P_2, ¶88) which corresponds to a first trusted party's public key (P_2 is the public element of ancestral PKG 304(b), ¶86, used in ¶88 to create $S_{z(n+1)}$), a third data set (ID_3, ¶86) that corresponds to a second identifier (ID_3 is identity information associated with the ancestral PKG 304(d), ¶¶85-86 ¶86 which is used in the creation of P_3, used in ¶88 to create $S_{z(n+1)}$) and a fourth data set (P_3, ¶88) which corresponds to a second trusted party's public key (P_3 is the public element of ancestral PKG 304(d), ¶86, used in ¶88 to create $S_{z(n+1)}$). Gentry is silent regarding a computer apparatus comprising a memory arranged to perform the key generation. However, Gentry '554 teaches a similar system (¶3) using entities and private key generators (¶22, Fig. 6) where the entities comprise a processor executing program code to carry out the cryptographic procedures described therein (¶¶40-42), allowing various entities to determine encryption keys (¶40) using a network (¶42). Therefore, it would have been obvious to one

having ordinary skill in the art at the time the invention was made to modify Gentry to carry out the cryptographic key generating procedures on a computer apparatus comprising a processor. One of ordinary skill in the art would have been motivated to perform such a modification to provide computer entities with a cryptographic key over a network, as taught by Gentry '554.

Regarding claim 2, Gentry discloses wherein the first and third data sets are public parameters (ID_2 and ID_3) are public parameters (identities are publicly known, for example, $P_3 = H_1(ID_1, ID_2, ID_3)$, ¶86).

Regarding claim 4, Gentry discloses wherein the second and fourth data sets (P_2 and P_3) are public parameters (public elements, ¶86).

Regarding claim 5, Gentry discloses wherein the second and fourth data sets (P_2 and P_3) are public parameters (public elements, ¶86).

Regarding claim 7, Gentry discloses wherein the first and second data sets (ID_2 and P_2) comprise a first common parameter (ID_2, ¶85, ¶86) associated with said first identity (PKG 304(b)) and said first trusted party (ancestral PKG 304(b); in Fig. 3, PKG 304(b) is second lower-level PKG in hierarchy, so P_{zi} of ¶86 is P_2, with respect to PKDG 304(b), and comprises $H_1(ID_1, ID_2)$), and the third and fourth data sets (ID_3 and P_3) comprise a second common parameter (ID_3, ¶85, ¶86) associated with said second identity (PKG 304(d)) and said second trusted party (ancestral PKG 304(d); in Fig. 3, PKG 304(d) is third lower-level PKG in hierarchy, so P_{zi} of ¶86 is P_3, with respect to PKDG 304(b), and comprises $H_1(ID_1, ID_2, ID_3)$).

Regarding claim 8, Gentry discloses wherein the cryptographic key (secret element) is an encryption key (secret element, encrypting/signing a message using the sender's (which is the same as the recipient in ¶¶85-95) secret element, ¶143).

Regarding claim 9, Gentry, as modified above, discloses wherein the processor is arranged to encrypt a fifth data set (message) with the encryption key (secret element, encrypting/signing a message using the sender's (which is the same as the recipient in ¶¶85-95) secret element, ¶143).

Regarding claim 10, Gentry, as modified, discloses wherein the processor is arranged to encrypted the fifth data set (message) with the encryption key (secret element, encrypting/signing a message using the sender's (which is the same as the recipient in ¶¶85-95) secret element, ¶143) and a random number (r, ¶95).

Regarding claim 11, Gentry discloses a method of generating a cryptographic key (key to recover V, i.e. $\prod_{i-2}^{n+1} \hat{e}(Q_{i-1}, U_i)$ where $U_i = rP_{zi}$, ¶95) using a first data set ($U_i = rP_{zi}$, ¶86) that corresponds to a first identifier ($P_{zi} = H_1(ID_1,...,ID_{zi})$, ¶86), a second data set that corresponds to a first trusted party's public key (ancestor's key generation parameter, Q_{i-1}, ¶89), a third data set ($U_i = rP_{zi}$ for the next ancestral PKG, ¶86) and a fourth data set that corresponds to a second party's public key (next ancestor's key generation parameter, Q_{i-1}, ¶89), wherein the cryptographic key is an encryption key (secret element, encrypting/signing a message using the sender's (which is the same as the recipient in ¶¶85-95) secret element, ¶143), wherein the processor is arranged to form said encryption key using a bilinear pairing operation (pairing

function ê, ¶64 & ¶66 & $\prod_{i-2}^{n+1} \hat{e}(Q_{i-1}, U_i)$, ¶95) on the first and second data sets ($\hat{e}(Q_{i-1}, U_i)$, *i*=first value, ¶95) and the third and fourth data sets ($\hat{e}(Q_{i-1}, U_i)$, *i*=next value, ¶95). Gentry is silent regarding a computer apparatus comprising a memory arranged to perform the key generation. However, Gentry '554 teaches a similar system (¶3) using entities and private key generators (¶22, Fig. 6) where the entities comprise a processor executing program code to carry out the cryptographic procedures described therein (¶¶40-42), allowing various entities to determine encryption keys (¶40) using a network (¶42). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Gentry to carry out the cryptographic key generating procedures on a computer apparatus comprising a processor. One of ordinary skill in the art would have been motivated to perform such a modification to provide computer entities with a cryptographic key over a network, as taught by Gentry '554.

Regarding claim 12, Gentry discloses wherein the bilinear mapping function (pairing function ê, ¶64 & ¶66) is either a Tate or Weil pairing (¶64).

Regarding claim 28, Gentry discloses a first entity (ancestral PKG 304(a), Fig. 3, #304a) arranged to generate a first data set (P_1, ¶86) that corresponds to a first trusted party's (ancestral PKG 304(a)) public key (P_1, ¶86), a second entity (ancestral PKG 304(b), Fig. 3, #304b) arranged to generate a second data set (P_2, ¶86) that corresponds to a second trusted party's (ancestral PKG 304(b)) public key (P_2, ¶86) and a third entity (ancestral PKG 304(d), Fig. 3, #304d & sender, Fig. 3, #306) arranged to generate a cryptographic key (recipient secret element, $S_{z(n+1)}$, i.e. the private key of the recipient, ¶90, where $z(n+1) = 4$) using a first

identifier (ID_1 , see equation for $P_{z(n+1)} = H_1(ID_{z1},...,ID_{z(n+1)})$, ¶90) in conjunction with the first data set (P_1 , see equation for $S_{z(n+1)}$, also called the Extraction algorithm, ¶90) and a second identifier (ID_2 , see equation for $P_{z(n+1)} = H_1(ID_{z1},...,ID_{z(n+1)})$, ¶90) in conjunction with the second data set (P_2 , see equation for $S_{z(n+1)}$, also called the Extraction algorithm, ¶90). Gentry is silent regarding the entities being computer entities in a computer system. However, Gentry '554 teaches a similar system (¶3) using entities and private key generators (¶22, Fig. 6) where the entities comprise a processor executing program code to carry out the cryptographic procedures described therein (¶¶40-42), allowing various entities to determine encryption keys (¶40) using a network (¶42). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Gentry to use computer entities in a computer system to carry out the out the cryptographic key generating procedures of the PKGs and recipient. One of ordinary skill in the art would have been motivated to perform such a modification to provide computer entities with a cryptographic key over a network, as taught by Gentry '554.

Regarding claim 29, Gentry discloses wherein the third computer entity (ancestral PKG 304(d), Fig. 3, #304d & sender, Fig. 3, #306) is arranged to encrypt a third data set (message) with the cryptographic key (secret element, encrypting/signing a message using the sender's (which is the same as the recipient in ¶¶85-95) secret element, ¶143).

Regarding claim 32, Gentry discloses wherein the first and second data sets are public parameters (P_1 and P_2) are public parameters (public elements for respective entities, ¶86).

Regarding claim 33, Gentry discloses that the public data parameters (P_1 and P_2) include an elliptic curve (G_1, group of points on an elliptic curve used to define the points, ¶64) and a generator point on the elliptic curve (each public element is a generator P, ¶65).

Regarding claim 43, the claim is substantially equivalent to claim 34 and is therefore rejected under similar rationale under Gentry. However, Gentry is silent regarding a computer apparatus comprising a memory arranged to perform the key generation. However, Gentry '554 teaches a similar system (¶3) using entities and private key generators (¶22, Fig. 6) where the entities comprise a processor executing program code to carry out the cryptographic procedures described therein (¶¶40-42), allowing various entities to determine encryption keys (¶40) using a network (¶42). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Gentry to carry out the cryptographic key generating procedures on a computing apparatus conditioned by a computer program product installed in the computing apparatus. One of ordinary skill in the art would have been motivated to perform such a modification to provide computer entities with a cryptographic key over a network, as taught by Gentry '554.

Allowable Subject Matter

14. Claims 30-31, 42 & 48 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Regarding claim 30, Gentry discloses bilinear pairing (¶¶64-66 & ¶95), but lacks encrypting using a bilinear pairing when operating on the first and third data sets and the second

and fourth data sets. Further, the prior art of record fails to teach or disclose, either alone or in combination, the above limitation in combination with the other elements of the claim.

Regarding claim 42, Gentry lacks wherein different trusted authorities are associated with different elements to which said bilinear mapping function can be applied, each trusted authority having an associated public key formed from its associated element and a secret of that trusted authority. Further, the prior art of record fails to teach or disclose, either alone or in combination, the above limitation in combination with the other elements of the claim.

Regarding claim 48, Gentry discloses wherein the user identity and trusted authority of each data set are each associated with a respective point on an elliptic curve (P_{zi} is generated using hash function H_1, which produces a point in G_1, the points on an elliptic curve (¶85) which is a group of points on an elliptic curve (¶64), and $Q_{zi} = s_{zi}P_o, 1 \le i \le n$, where P_o is a generator in G_1 (¶85)), the point associated with the user identity (P_{zi}, ¶86) is formed by a map-to-point hash function (H_1, ¶85) applied to the user identity (ID_{zi}, ¶86), the combination of this point with a secret (secret element, ¶88) of the trusted authority forming an identity-based private key (secret element, $S_{zi} = S_{z(i-1)} + s_{z(i-1)}P_{zi}$). However, the point associated with the trusted authority does not form, together with a combination of this point with a secret of the trusted authority, a public key of the trusted authority. Further, the prior art of record fails to teach or disclose, either alone or in combination, the above limitation in combination with the other elements of the claim.

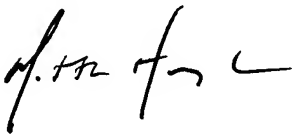
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS



May 7, 2007